Proceedings of the Edinburgh Mathematical Society (2010) **53**, 385–392 ©
DOI:10.1017/S0013091508000989 Printed in the United Kingdom

SQUARE-FREE VALUES OF QUADRATIC POLYNOMIALS

J. B. FRIEDLANDER[1] AND H. IWANIEC[2]

[1] *Department of Mathematics, University of Toronto, Toronto, Ontario M5S 2E4, Canada* (frdlndr@math.toronto.edu)
[2] *Department of Mathematics, Rutgers University, Piscataway, NJ 08903, USA*

(Received 29 September 2008)

Dedicated to the memory of George Greaves

Abstract We consider the quadratic polynomial $m^2 + D$ and study the asymptotic formula for the number of integers m, $1 \leqslant m \leqslant M$, for which the values of the polynomial are square-free. We are interested in particular in the question of how small we can take M in relation to D and still have the asymptotic hold.

Keywords: quadratic polynomial; square-free numbers

2010 *Mathematics subject classification:* Primary 11N32
Secondary 11N35

1. Introduction

George Greaves was greatly interested in the topic of sieve methods and contributed much to the subject (see, for example, his pioneering work on weighted sieves [**3**] and his monograph [**4**]). One particular aspect that attracted his attention from quite early on was the application of the sieve to problems involving the sequence of values of a polynomial (see, for example, [**2**]).

Among the easiest tasks that one can assign to a sieve is the counting of square-free numbers, a topic wherein even the original sieve ideas of Möbius inversion are useful in obtaining some interesting estimates. Almost the very simplest polynomials that could occur to one to study are quadratic polynomials in a single variable. Yet, even here, because the sequence of values of the polynomial is so lacunary, our knowledge is quite incomplete and some basic questions remain unanswered.

We consider the polynomial $m^2 + D$, restrict the variable to integers $1 \leqslant m \leqslant M$ and ask: for how many of these integers is the value of the polynomial square-free? The demonstration of the asymptotic formula for such polynomials was first established by Estermann [**1**], a result which, two years later, was greatly generalized by Ricci [**7**]. The problem of counting these integers becomes much more challenging when the quadratic polynomial has large coefficients and uniformity in these is wanted. We shall thus be concerned with the situation where M is relatively small compared with D.

It is easy to predict the asymptotic formula

$$\sum_{m\leqslant M}\mu^2(m^2+D)\sim cM, \tag{1.1}$$

where $c=c(D)$ is given by

$$c=\sum_d \mu(d)\rho(d^2)d^{-2}=\prod_p(1-\rho(p^2)p^{-2}), \tag{1.2}$$

and $\rho(q)$ denotes the number of solutions to $\nu^2+D\equiv 0\,(\mathrm{mod}\,q)$. Obviously, $\rho(p^2)\leqslant 2$ if $p^2\nmid D$ and $\rho(p^2)\leqslant p$ if $p^2\mid D$, so c is a positive constant.

2. A first result

Using Möbius inversion we get

$$\sum_{m\leqslant M}\mu^2(m^2+D)=\sum_d \mu(d)|\mathcal{A}_{d^2}|, \tag{2.1}$$

where

$$|\mathcal{A}_{d^2}|=\sum_{\substack{m\leqslant M,\\ m^2+D\equiv 0\,(\mathrm{mod}\,d^2)}} 1=\rho(d^2)d^{-2}M+O(\rho(d^2)). \tag{2.2}$$

For relatively small d this simple formula does the job. Indeed, we have

$$\sum_{d\leqslant Y}\rho(d^2)\ll\tau(D)Y\log Y, \tag{2.3}$$

which shows that (2.2) is valuable for $d\leqslant Y\ll MD^{-\varepsilon}$.

For larger d we do not need an asymptotic formula for $|\mathcal{A}_{d^2}|$, but need only a rough upper bound because the squares are so sparse that these terms can only contribute to the error term. However, establishing sufficient bounds is not easy if M is small. As one possible approach we can consider the congruence $m^2+D\equiv 0\,(\mathrm{mod}\,d^2)$ as the norm equation

$$d^2k-m^2=D \tag{2.4}$$

in the real quadratic field $\mathbb{Q}(\sqrt{k})$ and sum over $k\leqslant(D+M^2)Y^{-2}$, obtaining the bound

$$\sum_{d>Y}|\mathcal{A}_{d^2}|\ll\tau(D)(D+M^2)Y^{-2}\log 2DM. \tag{2.5}$$

Here, $\tau(D)$ comes from the estimation of the number of ideals of norm D and the logarithm comes from the estimation of the units. Hence, the total error term is

$$[MY^{-1}+Y+(D+M^2)Y^{-2}]\tau(D)\log 2DM, \tag{2.6}$$

where the first term comes from extending the sum in the main term to all $d>Y$. Taking $Y=(D+M^2)^{1/3}$, we arrive at the following result.

Theorem 2.1. *For any $D, M \geqslant 1$ we have*

$$\sum_{m \leqslant M} \mu^2(m^2 + D) = cM + O(\tau(D)(D + M^2)^{1/3} \log 2DM). \tag{2.7}$$

Note that (2.7) yields the true asymptotic for $M \geqslant D^{1/3+\varepsilon}$.

3. The square sieve

A different approach to (2.4) is to ask for the square values of $d^2k - D$ in the relatively short interval $[1, M^2]$. This combines two different objectives. The detection of integers in short intervals is amenable to standard Fourier analysis (which here amounts to counting the lattice points (d, k) in a narrow region). However, the detection of squares is not so standard. We shall employ the 'square sieve', which was introduced by Heath-Brown [**5**]. What we need from his method is the following.

Proposition 3.1. *For a_n with $n \geqslant 1$ non-negative reals and $P \geqslant 2$ we have*

$$\sum_{n=\square} a_n \leqslant 10P^{-2} \sum_n a_n \biggl(\biggl(\sum_{P<p\leqslant 2P} \biggl(\frac{n}{p}\biggr) \log p\biggr)^2 + (\log n)^2\biggr).$$

Here of course, (n/p) denotes the Legendre symbol.

Proof. Since the weights are non-negative, it suffices to check that these are $\geqslant 1$ on the square values $n = m^2$. Using the inequality $a^2 + 4b^2 \geqslant \frac{4}{5}(a+b)^2$ we find that

$$\begin{aligned}\biggl(\sum_{P<p\leqslant 2P} \biggl(\frac{n}{p}\biggr) \log p\biggr)^2 + (\log m^2)^2 &\geqslant \frac{4}{5}\biggl(\sum_{\substack{P<p\leqslant 2P,\\ p\nmid m}} \log p + \log m\biggr)^2 \\ &\geqslant \frac{4}{5}\biggl(\sum_{P<p\leqslant 2P} \log p\biggr)^2 \\ &\geqslant \frac{P^2}{10},\end{aligned}$$

which completes the proof. $\square$

Using this square sieve we can sharpen the bound (2.5) and improve (2.7) to the following.

Theorem 3.2. *For $1 \leqslant M \leqslant D$ we have*

$$\sum_{m \leqslant M} \mu^2(m^2 + D) = cM + O(\tau(D)M^{3/5}D^{1/10}(\log 2D)^2). \tag{3.1}$$

Note that (3.1) is a meaningful asymptotic formula for $M \geqslant D^{1/4+\varepsilon}$.

https://doi.org/10.1017/S0013091508000989 Published online by Cambridge University Press

4. Proof of Theorem 3.2

It suffices to establish the result (3.1) for the sum over the dyadic segments $M < m \leqslant 2M$. We can also assume that

$$D^{1/4} \leqslant 4M \leqslant D^{1/2},$$

since otherwise the result either is trivial or follows from (2.7). We shall prove that

$$\sum_{d>Y} |\mathcal{A}_{d^2}| \ll \tau(D)\biggl(\frac{MD^{1/6}}{Y^{2/3}} + \frac{D^{1/3}}{Y^{1/3}} + \frac{D^{1/2}}{M} + \frac{M^2}{Y^2} + \frac{M^{4/3}}{D^{1/3}}\biggr)(\log D)^2, \tag{4.1}$$

which is somewhat better than (2.5) and which, when combined with (2.3), gives (3.1) on choosing $Y = M^{3/5}D^{1/10}$.

For the proof of (4.1) we also divide the range of d into dyadic segments $\Delta < d \leqslant 2\Delta$ with

$$Y \leqslant \Delta \leqslant D^{1/2}. \tag{4.2}$$

Now, by the square sieve we obtain

$$\sum_{\Delta<d\leqslant 2\Delta} |\mathcal{A}_{d^2}| \leqslant 10P^{-2} \mathop{\sum\sum}_{\substack{\Delta<d\leqslant 2\Delta,k\\ M^2<|kd^2-D|\leqslant 4M^2}} [\cdots] \tag{4.3}$$

where the content of $[\cdots]$ is given by

$$\biggl(\sum_{P<p\leqslant 2P}\biggl(\frac{kd^2-D}{p}\biggr)\log p\biggr)^2 + (4\log 2M)^2.$$

Here we can make the restriction $p \nmid dD$ at the cost of an extra term $O((\log D)^2)$. Next, before opening the square, we introduce two smoothing factors $\eta(d)\xi(kd^2 - D)$, where $\eta(v)$ and $\xi(u)$ are smooth functions supported on $v \asymp \Delta$ and $u \asymp M^2$, respectively, with $v^j\eta^{(j)}(v) \ll 1$ and $u^j\xi^{(j)}(u) \ll 1$ for $j = 0, 1, \dots, 4$. Then (4.3) yields

$$\sum_{\Delta<d\leqslant 2\Delta} |\mathcal{A}_{d^2}| \ll \biggl(\frac{\log P}{P}\biggr)^2 \mathop{\sum\sum}_{\substack{P<p_1\neq p_2\leqslant 2P,\\ (p_1p_2,D)=1}} |S_{p_1p_2}| + \frac{(\log D)^2}{P}S_1, \tag{4.4}$$

where

$$S_q = \sum_{(d,q)=1}\sum_{k}\eta(d)\xi(kd^2-D)\biggl(\frac{kd^2-D}{q}\biggr).$$

Next we evaluate S_q using Poisson's Formula:

$$S_q = \frac{1}{q^2}\sum_{h}\sum_{\ell} F\biggl(\frac{h}{q},\frac{\ell}{q}\biggr)G_q(h,\ell), \tag{4.5}$$

where $F(x,y)$ is the Fourier integral

$$F(x,y) = \iint \eta(v)\xi(uv^2-D)e(-xu-yv)\,\mathrm{d}u\,\mathrm{d}v \tag{4.6}$$

and $G_q(h,\ell)$ is the complete character sum

$$G_q(h,\ell)=\sum_{\alpha(q)}\sideset{}{^*}\sum_{\beta(q)}\Big(\frac{\alpha\beta^2-D}{q}\Big)e\Big(\frac{\alpha h+\beta\ell}{q}\Big). \tag{4.7}$$

To estimate $F(x,y)$ we make a change of variable and write

$$F(x,y)=\iint\eta(v)\xi(u)e\Big(-x\frac{u+D}{v^2}-yv\Big)\frac{\mathrm{d}u\,\mathrm{d}v}{v^2}.$$

Integrating by parts in the v-variable (zero or four times) and then estimating trivially in each variable, we derive

$$F(x,y)\ll\frac{M^2}{\Delta}\Big(1+\frac{|x|D}{\Delta^2}+|y|\Delta\Big)^{-4}\ll\frac{M^2}{\Delta}\Big(1+\frac{|x|D}{\Delta^2}\Big)^{-2}(1+|y|\Delta)^{-2}. \tag{4.8}$$

This estimate is valid for all x, y except in the region

$$|x|D\asymp|y|\Delta^3,\qquad xy\neq0. \tag{4.9}$$

In this range the exponential function may have a stationary point at $2xDv^{-3}=y$, so partial integration in the v-variable is not possible. But we can integrate by parts with respect to the u-variable (zero or two times). Having done so, we apply the second derivative test (say, [**8**, Lemma 4.5] or [**6**, Lemma 8.10]) and estimate trivially in the u-variable, obtaining

$$F(x,y)\ll\frac{M^2}{\Delta^2}\Big(1+\frac{|x|M^2}{\Delta^2}\Big)^{-2}\Big(\frac{\Delta^4}{|x|D}\Big)^{1/2}=\frac{M^2}{(|x|D)^{1/2}}\Big(1+\frac{|x|M^2}{\Delta^2}\Big)^{-2}. \tag{4.10}$$

We shall apply (4.8) and (4.10) for $(x,y)=(h/q,\ell/q)$ and sum these estimates for $|F(h/q,\ell/q)|$ over all integers h,ℓ. However, before being able to execute such a summation we require a bound for $G_q(h,\ell)$ for each $q=p_1p_2$. Since our estimates for the Fourier integrals do not depend specifically on q but only on its order of magnitude ($q=1$ or $q\asymp P^2$) we may first deal with

$$E(h,\ell)=\sum\sum_{\substack{P<p_1\neq p_2\leqslant 2P,\\(p_1p_2,D)=1}}|G_{p_1p_2}(h,\ell)|. \tag{4.11}$$

As a matter of fact, we could estimate every one of the individual sums $G_q(h,\ell)$ by an appeal to the Riemann Hypothesis for curves (Weil's bound for suitable character sums). However, we can do the job elementarily by taking advantage of the particular averaging over $p_1\neq p_2$.

Using the twisted multiplicativity

$$G_{p_1p_2}(h,\ell)=G_{p_1}(\bar{p}_2h,\bar{p}_2\ell)G_{p_2}(\bar{p}_1h,\bar{p}_1\ell),$$

by Cauchy's inequality we derive

$$E(h,\ell) \leqslant 2 \sum_{\substack{P<p\leqslant 2P,\\ p\nmid D}} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, p)} |G_p(ah,a\ell)|^2.$$

For the sum of prime modulus we have

$$G_p(h,\ell) = G_p(h) K_p(hD,\ell),$$

where

$$G_p(h) = \sum_{\alpha(p)} \left(\frac{\alpha}{p}\right) e\left(\frac{\alpha h}{p}\right) = \varepsilon_p \sqrt{p} \left(\frac{h}{p}\right)$$

is the Gauss sum and

$$K_p(h,\ell) = \sideset{}{^*}\sum_{\beta(p)} e\left(\frac{\beta^2 h + \bar{\beta}\ell}{p}\right)$$

is a hybrid Gauss–Kloosterman sum. We may assume $p \nmid hD$ and compute as follows:

$$\sideset{}{^*}\sum_{a(p)} |G_p(ah,a\ell)|^2 = p \sideset{}{^*}\sum_{a(p)} |K_p(ahD,a\ell)|^2 \leqslant \nu(h,\ell) p^2,$$

where $\nu(h,\ell)$ is the number of solutions of

$$(\beta_1^2 - \beta_2^2) hD + (\bar{\beta}_1 - \bar{\beta}_2)\ell \equiv 0 \,(\mathrm{mod}\, p)$$

in $\beta_1, \beta_2 \,(\mathrm{mod}\, p)$, $(\beta_1\beta_2, p) = 1$. There are $p-1$ solutions if $\beta_1 \equiv \beta_2$. For $\beta_1 \not\equiv \beta_2$ we have

$$(\beta_1 + \beta_2)\beta_1\beta_2 \equiv \ell\overline{hD} \,(\mathrm{mod}\, p).$$

After a change of variables we need to count the solutions of

$$\gamma(\gamma+1)\beta^2 \equiv \ell\overline{hD} \,(\mathrm{mod}\, p)$$

in $(\beta\gamma, p) = 1, \gamma \not\equiv 1$. If $p \mid \ell$, then $\gamma \equiv -1 \,(\mathrm{mod}\, p)$ and we get exactly $p-1$ solutions. If $p \nmid \ell$, then the number of solutions is equal to

$$\begin{aligned}\sum_{\gamma \not\equiv 0,\pm 1} \left(1 + \left(\frac{\ell hD\gamma(\gamma+1)}{p}\right)\right) &= p - 3 + \left(\frac{\ell hD}{p}\right) \sum_{\gamma \not\equiv 1} \left(\frac{\gamma(\gamma+1)}{p}\right) \\ &= p - 3 - \left(\frac{\ell hD}{p}\right)\left(1 + \left(\frac{2}{p}\right)\right) \\ &\leqslant p - 1.\end{aligned}$$

Summing the above counts, we find that $\nu(h,\ell) \leqslant 2(p-1)$. Hence, we conclude as follows.

Lemma 4.1. *For all h, ℓ we have*

$$E(h,\ell) \leqslant 16P^4. \tag{4.12}$$

https://doi.org/10.1017/S0013091508000989 Published online by Cambridge University Press

Since the bound (4.12) does not depend on h or ℓ, we can sum the estimates (4.8), (4.10) for $|F(h/q, \ell/q)|$ for $q = 1$ and $q \asymp P^2$ without any conditions on the frequencies h, ℓ. We obtain

$$\sum_h \sum_\ell |F(h/q, \ell/q)| \ll \frac{M^2}{\Delta} \sum_h \left(1 + \frac{|h|D}{q\Delta^2}\right)^{-2} \sum_\ell \left(1 + \frac{|\ell|\Delta}{q}\right)^{-2} + M^2 \sum_{\substack{|h|D \asymp |\ell|\Delta^3,\\ h\ell \neq 0}} \left(1 + \frac{|h|M^2}{q\Delta^2}\right)^{-2} \left(\frac{q}{|h|D}\right)^{1/2}.$$

On the right-hand side the first sum (over h) is $\ll (1 + q\Delta^2 D^{-1})$, the second sum (over ℓ) is $\ll (1 + q\Delta^{-1})$ and the third sum (over $h\ell \neq 0$) is bounded by

$$M^2 (qD)^{1/2} \Delta^{-3} \sum_h \left(1 + \frac{|h|M^2}{q\Delta^2}\right)^{-2} |h|^{1/2} \ll q^2 D^{1/2} M^{-1}.$$

Hence, we conclude as follows.

Lemma 4.2. *We have*

$$\sum_h \sum_\ell |F(h/q, \ell/q)| \ll \frac{M^2}{\Delta}\left(1 + \frac{q\Delta^2}{D}\right)\left(1 + \frac{q}{\Delta}\right) + q^2 \frac{D^{1/2}}{M}. \tag{4.13}$$

Now, combining (4.12) and (4.13), we get by (4.4) and (4.5)

$$\begin{aligned}\sum_{\Delta < d \leqslant 2\Delta} |\mathcal{A}_{d^2}| &\ll \frac{(\log D)^2}{P^2}\left[\frac{M^2}{\Delta}\left(1 + \frac{P^2\Delta^2}{D}\right)\left(1 + \frac{P^2}{\Delta}\right) + P^4 \frac{D^{1/2}}{M}\right] \\ &\quad + \frac{(\log D)^2}{P}\left[\frac{M^2}{\Delta}\left(1 + \frac{\Delta^2}{D}\right)\left(1 + \frac{1}{\Delta}\right) + \frac{D^{1/2}}{M}\right] \\ &\ll \left(\frac{M^2}{\Delta P} + P^2 \frac{D^{1/2}}{M} + \frac{M^2}{\Delta^2} + \frac{M^2\Delta}{D}\right)(\log D)^2.\end{aligned}$$

We choose $P = 2 + M(\Delta D^{1/2})^{-1/3}$ and the bound becomes

$$\ll (M D^{1/6} \Delta^{-2/3} + D^{1/3}\Delta^{-1/3} + D^{1/2} M^{-1} + M^2 \Delta^{-2} + M^2 \Delta D^{-1})(\log D)^2.$$

Here we improve the last term, $M^2\Delta D^{-1}$, by combining it with $D\Delta^{-2}$ in (2.5), obtaining $\min\{M^2\Delta D^{-1}, D\Delta^{-2}\} \leqslant M^{4/3} D^{-1/3}$. Having done so, we can see that the worst case for Δ is its smallest value, $\Delta = Y$, giving (4.1). This completes the proof of Theorem 3.2.

Acknowledgements. J.B.F. was supported in part by NSERC Grant no. A5123. H.I. was supported in part by NSF Grant no. DMS-08-02246.

References

1. T. Estermann, Einige Sätze über quadratfreie Zahlen, *Math. Annalen* **105** (1931), 653–662.
2. G. Greaves, Large prime factors of binary forms, *J. Number Theory* **3** (1971), 35–59.
3. G. Greaves, A weighted sieve of Brun's type, *Acta Arith.* **40** (1981), 297–332.
4. G. Greaves, *Sieves in number theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Volume 43 (Springer, 2001).
5. D. R. Heath-Brown, The square sieve and consecutive square-free numbers, *Math. Annalen* **266** (1984), 251–259.
6. H. Iwaniec and E. Kowalski, *Analytic number theory*, Colloquium Publications, Volume 53 (American Mathematical Society, Providence, RI, 2004).
7. G. Ricci, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo* **57** (1933), 433–475.
8. E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd edn (Clarendon Press, Oxford, 1986).